U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.256
May 21, 1999

DEPARTMENTAL GUIDE TO PERSONNEL SECURITY PLANNING

TABLE OF CONTENTS

DEPARTMENTAL GUIDE
TO
PERSONNEL SECURITY PLANNING

1. PURPOSE

The purpose of this Guide is to provide Department of Transportation (DOT) and their Operating Administration managers, ISSO's and network administrators with a step-by-step approach for developing a personnel security capability within their organizations.

2. SCOPE

The provisions of this Guide apply to the Department of Transportation (DOT), its Secretarial Offices and Operating Administrations.

3. GOALS

The Goal of personnel security planning is to improve the security of DOT information systems by guarding against potential damage caused by the intentional or unintentional actions of employees, contractors or the general public.

4. REFERENCES

The DOT Departmental Information Resources Management Manual (DIRMM) DOT H 1350.2 implements statutory and regulatory Information Resources Management (IRM) and security requirements for the Department. It also calls for ensuring the confidentiality, integrity, and availability of information contained, processed, or transmitted in/on sensitive systems. Refer to DOT H 1350.2.1 *Regulatory and Guidance Documents* for specific references.

5. OVERVIEW OF PERSONNEL SECURITY

Most security problems, whether accidental or malicious, begin with people. Of these people, by far, most of them come from within the organization. The foundation for dealing with people problems, therefore, is to try to eliminate the potential for problems before they happen. In order to address personnel security in a proactive fashion, plans should be created for the staffing of positions that interact with DOT information systems, the administration of users on such systems (including considerations for terminating employee access), and special considerations that may arise when contractors or the public have access to DOT information systems.

There are 2 major elements of personnel security that must be considered during the planning activity, --- Staffing and User Administration. The staffing process generally involves at least four steps and can apply equally to general users as well as to application managers, system management personnel, and security personnel. These four steps include defining the job, (normally involving the development of a position description), determining the sensitivity of the position, filling the position (which involves screening applicants and selecting an individual), and training the new individual. Effective administration of users' access to DOT information systems is also essential in implementing an overall Information System Security Program. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing (periodically verifying the legitimacy of current accounts and access authorizations). Finally, there are considerations involved in the timely modification or removal of access and associated issues for employees who are reassigned, promoted, or terminated, or who retire.

In addition to these two major elements, personnel security planning should also take into account security considerations when Contractors are allowed access to DOT information systems, and, similarly, when the public is granted access to certain information, generally via the Internet.

6. STAFFING

An organization's staffing process should pay particular attention to security at each point in the hiring and employee orientation process. To do this, specific security controls should be incorporated within the overall staffing process, as defined in the ensuing paragraphs.

A. Position Definition

Early in the process of defining a position, security issues should be identified and addressed. Once a position has been broadly defined, the responsible supervisor should determine the type of computer access needed for the position. There are two general security rules to apply when granting access, **---** separation of duties and least privilege.

- <u>Separation of Duties</u> **-** refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment. In effect, checks and balances need to be designed into both the process as well as the specific, individual positions of personnel who will implement the process.

- <u>Least Privilege</u> **-** refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database. However, least privilege does not mean that all users will have extremely little functional access; some employees will have significant access if it is required for their position. However, applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources. It is important to make certain that the implementation of least privilege does not interfere with the ability to have personnel substitute for each other without undue delay. Without careful planning, access control can interfere with contingency plans.

B. Determining Position Sensitivity

Various levels of sensitivity are assigned to positions in the federal government. Determining the appropriate sensitivity level is based upon such factors as the type and degree of harm (e.g., disclosure of private information, interruption of critical processing, computer fraud) the individual can cause through misuse of the information system, as well as more traditional factors (such as access to classified information and fiduciary responsibilities). The responsible manager should determine the position sensitivity, based on the duties and access levels, so that appropriate cost-effective screening can be completed.

It is important to carefully select the appropriate position sensitivity, since controls in excess of the sensitivity of the position waste resources, while too little control may result in unacceptable risks to the system.

C. Screening

Background screening helps to determine whether a particular individual is suitable for a given position. In the federal government, the screening process is formalized through a series of background checks conducted through a central investigative office within the organization or through another organization (e.g., the Office of Personnel Management). Within the Federal Government, the most basic screening technique involves a check for a criminal history, checking FBI fingerprint records, and other federal indices. More extensive background checks examine other factors, such as a person's work and educational history, personal interview, history of possession or use of illegal substances, and interviews with current and former colleagues, neighbors, and friends. The exact type of screening that takes place depends upon the sensitivity of the position and applicable DOT implementing regulations. The prospective employee's manager does not conduct screening; rather, agency security and personnel officers should be consulted for agency-specific guidance.

D. Employee Training and Awareness

Once an employee has been hired, it is important to perform sufficient indoctrination in the area of information protection to ensure a clear understanding of the policies to be adhered to, the procedures for adherence, and what happens in the case of non adherence. In many organizations, this information is not made clear from the outset, and is the basis for misunderstanding on all sides. Proper training is also necessary to assure that the employee is competent to carry out the procedures required to implement protection policies. Refer to DOT H 1350.258 *Departmental Guide to Developing an Information System Security Awareness/Training/Education Program* for additional guidance on this issue.

6. USER ADMINISTRATION

Effective administration of users' computer access is essential to maintaining information system security. Hence effective personnel security planning should ensure effective administration of users' computer access, --- including user account management, auditing and the timely modification or removal of access. The following should be considered:

A. User Account Management

Management of user accounts includes processes for requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions.

Establishing a user account typically begins with a request from the user's supervisor to the system administrator (SA) for a system account. If a user is to have access to a particular major application, this request may be sent through the application manager to the SA. This will ensure that the systems office receives formal approval from the application manager for the employee to be given access. The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile.

The SA will then use the account request to create an account for the new user. The access levels of the account will be consistent with those requested by the user's supervisor, and by various application managers. Next, employees will be given their account information, including the account identifier (e.g., user ID) and a means of authentication (e.g., password or smart card/PIN). Note that when employees are given their account, the process should include training and awareness on information security issues (Refer to DOT H 1350.258 *Departmental Guide to Developing an Information System Security Awareness/Training/Education Program*). In addition, users should be asked to review a set of rules and regulations for system access.

When user accounts are no longer required, the user's supervisor should inform the SA and the appropriate application manager(s), so that these accounts can be removed in a timely manner. Further termination issues are discussed in Paragraphs D and E of this Section.

It is important to note that access and authorization administration is a continuing process. New user accounts are continually being added, while others are deleted. In addition, permissions may change, --- sometimes permanently, sometimes only temporarily. New applications may be added, upgraded, and removed, with changing lists of authorized users. Tracking this information to keep it up to date is essential to allow users access to only those functions necessary to accomplish their assigned responsibilities.

One significant aspect of user account management involves keeping user access authorizations up to date. Access authorizations are typically changed under two types of circumstances, --- a change in job role, either temporarily (e.g., while covering for an employee on sick leave) or permanently (e.g., after an in-house transfer), and termination (discussed in Paragraphs D and E of this Section).

Users often are required to perform duties outside their normal scope during the absence of others. This requires additional access authorizations. Although necessary, such extra access authorizations should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes. Also, they should be removed promptly when no longer required.

Permanent changes are usually necessary when employees change positions within an organization. In this case, the process of granting account authorizations will occur again. At this time, however, is it also important that access authorizations of the prior position be removed. Many instances of "authorization creep" have occurred with employees continuing to maintain access rights for previously held positions within the organization. This practice is inconsistent with the principle of least privilege.

B. Audit and Management Reviews

It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels, --- on an application-by-application basis, or on a system wide basis. A good practice is for application managers (and data owners, if different) to review all access levels of all application users every month. Whereas the SA can verify that users only have those accesses that their managers have specified, because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.

C. Detecting Unauthorized/Illegal Activities

Mechanisms besides auditing and analysis of audit trails should be used to detect unauthorized and illegal acts. Rotating employees in sensitive positions, which could expose a scam that required an employee’s presence or periodic re-screening of personnel are methods that can be used.

D. Friendly Termination

Friendly termination refers to the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Since terminations can be expected regularly, this is usually accomplished by implementing a standard set of procedures for outgoing or transferring employees. These are part of the standard employee "out-processing," and are put in place to ensure that system accounts are removed in a timely manner. This normally includes:

- removal of access privileges, computer accounts, authentication tokens,

- the control of keys,
- the briefing on the continuing responsibilities for confidentiality and privacy,
- return of property, and
- continued availability of data. In both the manual and the electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how are they backed up. Employees should be instructed whether or not to "clean up" their PC before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.

E. Unfriendly Termination

Unfriendly termination involves the removal of an employee under involuntary or adverse conditions. This may include termination for cause, Reduction in Force (RIF), involuntary transfer, resignation for "personality conflicts," and situations with pending grievances. The tension in such terminations may multiply and complicate security issues. Additionally, all of the issues involved in friendly terminations are still present, but addressing them may be considerably more difficult.

The greatest threat from unfriendly terminations is likely to come from those personnel who are capable of changing code or modifying the system or applications. For example, systems personnel are ideally positioned to wreak considerable havoc on systems operations. Without appropriate safeguards, personnel with such access can place logic bombs (e.g., a hidden program to erase a disk) in code that will not even execute until after the employee's departure. Backup copies can be destroyed. There are even examples where code has been "held hostage." But other employees, such as general users, can also cause damage. Errors can be input purposefully, documentation can be mis-filed, and other "random" errors can be made. Correcting these situations can be extremely resource intensive. Given the potential for adverse consequences, organizations should do the following:

- System access should be terminated as quickly as possible when an employee is leaving a position under less than friendly terms. If an employee is to be fired, system access should be removed at the same time (or just before) the employee is notified of his/her dismissal.
- When an employee notifies an organization of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated.
- During the "notice of termination" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.
- In some cases, physical removal from the offices may be necessary.

7. CONTRACTOR ACCESS CONSIDERATIONS

DOT utilizes contractors and consultants to assist with a wide variety of information technology taskings. In cases where these individuals perform their taskings at a DOT facility, access to DOT information systems is often a necessity. Hence consultant/contractor access must be accounted for in the personnel security planning process. In addition, these individuals must be made aware of applicable DOT security policy and procedures, by providing them with DOT H 1350.273 *Guide to Information Protection for Contractors*.

8. PUBLIC ACCESS CONSIDERATIONS

Like other federal agencies, DOT utilizes electronic methods, such as the Internet, for electronic dissemination of information to the public. When DOT systems are made available for access by the public (or a large or significant subset thereof), it triggers additional security issues, based upon the increased risk. Public access systems are subject to a threat from hacker attacks on the confidentiality, availability, and integrity of information processed by a system. Besides increased risk of hackers, public access systems can also be subject to insider malice. For example, an unscrupulous user, such as a disgruntled employee, may try to introduce errors into data files intended for distribution in order to embarrass or discredit the organization. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public confidence due to the high visibility of public access systems. Other security problems may arise from unintentional actions by untrained users. Hence, when opening up a system to public access, additional precautions may be necessary because of the increased threats.